

## SECURE SYSTEM FOR ACTIVATING PERSONAL COMPUTER SOFTWARE AT REMOTE LOCATIONS

Patent number: JP6501120T

Publication date: 1994-01-27

Inventor:

Applicant:

Classification:

- international: G06F13/00; G06F15/00; H04L9/00; H04L9/00;  
H04L9/10; H04L9/12

- european: G06F1/00N7R2; G06F9/445; G06F9/445N;  
G06F21/00N7P5M

Application number: JP19910501845T 19911106

Priority number(s): US19900610037 19901107; US19910682456 19910409

Also published as:



WO9209160 (A1)



EP0556305 (A1)



US5222134 (A1)



EP0556305 (A4)



EP0556305 (B1)

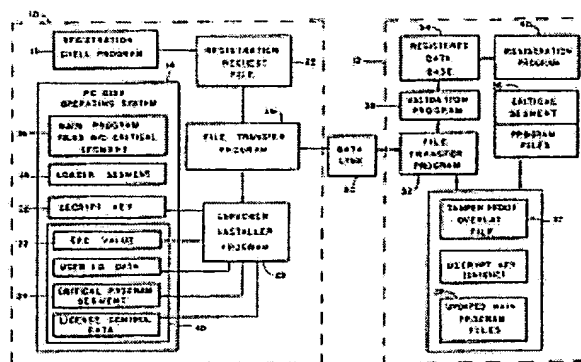
more >>

Report a data error here

Abstract not available for JP6501120T

Abstract of corresponding document: **US5222134**

A process and system for activating various programs are provided in a personal computer. The computer is initially provided with a registration shell. A data link is established between the personal computer and a registration computer. By providing the registration computer with various information, a potential licensee can register to utilize the program. Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer and transferred to the personal computer. The tamperproof overlay includes critical portions of the main program, without which the main program would not operate and also contains licensee identification and license control data.



Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平6-501120

第6部門第3区分

(43) 公表日 平成6年(1994)2月3日

(51) Int.Cl. <sup>4</sup>	識別記号	序内整理番号	F I
G 0 6 F 13/00	3 5 1 H	7368-5B	
15/00	3 3 0 A	7459-5L	
H 0 4 L 9/00			
9/10			
	7117-5K	H 0 4 L 9/00	Z
	審査請求 有	予備審査請求 有	(全 8 頁) 最終頁に続く

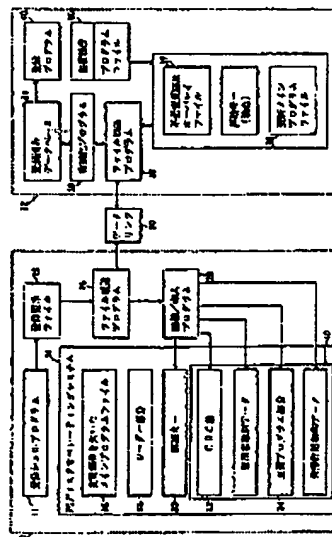
(21) 出願番号 特願平4-501845  
 (86) (22) 出願日 平成3年(1991)11月6日  
 (85) 翻訳文提出日 平成5年(1993)5月7日  
 (86) 国際出願番号 P C T / U S 9 1 / 0 8 0 6 9  
 (87) 国際公開番号 W O 9 2 / 0 9 1 6 0  
 (87) 国際公開日 平成4年(1992)5月29日  
 (31) 優先権主張番号 6 1 0 , 0 3 7  
 (32) 優先日 1990年11月7日  
 (33) 優先権主張国 米国 (U S)  
 (31) 優先権主張番号 6 8 2 , 4 5 6  
 (32) 優先日 1991年4月9日  
 (33) 優先権主張国 米国 (U S)

(71) 出願人 タウ システム コーポレーション  
 アメリカ合衆国 バージニア州 フォルス  
 チャーテ, リースバーグ バイク,  
 7115, スーツ327  
 (72) 発明者 ワイト, デービッド, ビー  
 アメリカ合衆国 バージニア州 22032,  
 フェアファックス ギルバートソン ロー  
 ド, 4220  
 (72) 発明者 リッデル, ホレイス, ジー  
 アメリカ合衆国 バージニア州 22021,  
 チャンチリイ, バレイ カウントリ ドラ  
 イブ, 13811  
 (74) 代理人 弁護士 倉持 裕 (外1名)  
 最終頁に続く

(54) 【発明の名称】 パーソナルコンピュータのソフトウェアを遠隔位置で起動するための安全システム

## (57) 【要約】

様々なプログラムを起動するための過程とシステムがパーソナルコンピュータ(10)に提供されている。パーソナルコンピュータ(10)には、登録シェプログラム(11)が当初備わっている。データリンク(30)がパーソナルコンピュータ(10)と登録用コンピュータ(12)の間に確立される。登録用コンピュータ(12)に様々な情報を与えることにより、見込み被許者はメインプログラム(16)の使用を登録することができる。ひとたび登録過程が完了すると、不正変更防止オーバーレイプログラムが登録用コンピュータ(12)において作成され、パーソナルコンピュータ(10)に転送される。不正変更防止オーバーレイには、メインプログラム(16)の主要部分がふくまれ、これを欠くとメインプログラム(16)は動作せず、また不正変更防止オーバーレイには使用許識別データと使用許制御データも含まれている。



## 【請求の範囲】

1. プログラムファイルを起動する方法であって、  
 住所記憶を有する遠隔コンピュータに対して、ローダーセグメントと登録シェル部分を含むプログラムファイルを提供し、上記プログラムファイルは必要部分を欠いて、上記プログラムファイルを正しく実行することを防止する工程、  
 使用者識別情報を上記登録シェル部分に入力する工程、  
 上記使用者識別情報を、上記登録シェルから登録用コンピュータ内にある独立した登録プログラムに転送し、上記登録プログラムは使用者識別データと上記必要部分とを結合して独自のオーバーレイファイルを作成する工程、  
 上記独自のオーバーレイファイルを上記登録プログラムから上記登録シェルに転送する工程、上記オーバーレイファイルには上記プログラムファイルには記載されていない必要部分が含まれ、そして  
 上記オーバーレイファイルを上記メインプログラムファイルに導入する工程を有し、上記オーバーレイファイルに入っている使用者識別が導入されたときだけ上記プログラムファイルの動作を可能とすることを特徴とする前記のプログラムファイル起動方法。
2. 上記オーバーレイファイルを上記登録用コンピュータから上記遠隔コンピュータに転送する前に、上記使用者識別情報を利用可能にする工程を有する請求の範囲第1項に記載の方法。
3. 不正変更防止のオーバーレイファイルを作成する工程を有する請求の範囲第1項に記載の方法。
4. 上記不正変更防止オーバーレイファイルが上記オーバーレイファイルを暗号化することにより作成され、遠隔冗長検査値が上記

主要プログラム部分が欠けているプログラムファイルが自動的に検出されていて、このプログラムファイルが動作することを防止し、上記オーバーレイローダー部分は本物のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記遠隔コンピュータには登録シェルプログラムが備えられ、上記登録シェルプログラムは使用者が様々な使用者識別情報を入力することを可能にするような少なくとも一台の遠隔コンピュータと、

登録プログラムと、上記使用者識別情報を受渡し処理するための手段と、上記プログラムファイルに欠けている上記主要プログラム部分と使用者識別情報の全部あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに転送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記遠隔コンピュータに転送することで、上記オーバーレイファイルに入っている使用者識別が現在導入されているときだけ上記プログラムファイルの動作が可能になることを特徴とする上記プログラムファイル起動システム。

13. 上記遠隔コンピュータと上記登録用コンピュータとの間を結合する電子データリンクと、上記登録用コンピュータと上記遠隔コンピュータの両方に備えられているファイル転送処理とを含むことを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

12. 上記登録用コンピュータが、すべての登録済み使用者が含まれている中央データベースと上記使用者識別情報を蓄積するための手段とを備えていることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

## 特開平6-501120 (2)

暗号化オーバーレイファイル内にあるとともに、暗号キーを上記オーバーレイファイルに埋する請求の範囲第8項に記載の方法。

5. 上記オーバーレイが実行のためにロードされるたびに遠隔冗長検査値が計算され、上記不正変更防止オーバーレイファイル内に転送された遠隔冗長検査値と比較され、上記オーバーレイファイルが作成以後変更されているかどうかを判断することを特徴とする請求の範囲第1項に記載の方法。

6. 上記使用者識別情報と上記オーバーレイファイルとが、電子データリンクを介して上記登録シェルと上記登録プログラムとの間を転送されることを特徴とする請求の範囲第1項に記載の方法。

7. 上記登録シェルプログラムが、上記の独立した登録用コンピュータを備えた少なくとも二台の遠隔コンピュータから離れた、第一のコンピュータ内に埋されていることを特徴とする請求の範囲第1項に記載の方法。

8. 上記利用可能工程によって上記使用者識別情報が正式の登録シェルを確保することを特徴とする請求の範囲第1項に記載の方法。

9. 上記使用者識別と上記オーバーレイファイルが、一台のコンピュータに入力され備えられることを特徴とする請求の範囲第1項に記載の方法。

10. プログラムファイルを削除されたもしくは削除されない期間を測定するためのシステムにおいて、  
 オーバーレイローダー部分が含まれているが少なくとも一つの

13. オーバーレイファイルを作成するための上記手段が、遠隔冗長検査値を備える不正変更防止オーバーレイファイルを作成するための暗号化装置と暗号キーを備えており、上記暗号キーは上記オーバーレイファイルと共に上記遠隔コンピュータに転送されることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

14. 上記遠隔コンピュータが、上記オーバーレイファイルを解除し、上記オーバーレイファイルが実行のためにロードされるたびに遠隔冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータによって上記オーバーレイファイルと共に転送された遠隔冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第12項に記載のプログラムファイル起動システム。

15. 上記必要部分がエグゼクティブ制御部分であり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第1項に記載の方法。

16. 上記主要プログラム部分のエグゼクティブ制御プログラムであり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

17. 上記必要部分がエグゼクティブ制御プログラム部分がプログラムファイル全体を有することを特徴とする請求の範囲第16項に記載のプログラムファイル起動システム。

18. プログラムファイルの使用を制御する方法において、  
 住所記憶を有するコンピュータに対してローダー部分と登録シェル部分を含むプログラムファイルを提供し、上記プログラムフ

特表平6-501120 (9)

ファイルは第一レベルの制御機能を実行するエグゼクティブ制御プログラムを有しており、

情報を上記登録シェル部分に入力し、

上記使用許諾契約情報を上記登録シェルから独立登録プログラムに伝送し、上記登録プログラムは使用許諾契約データを第二レベルの制御機能を有するエグゼクティブ制御プログラムに結合して独自のオーバーレイファイルを作成し、

上記独自のオーバーレイファイルを上記登録プログラムから上記登録シェルに伝送し、上記オーバーレイファイルには上記第二レベルのエグゼクティブ制御プログラムが含まれており、そして

上記独自のオーバーレイファイルを上記主要プログラムファイルに導入し、上記プログラムファイルの第二レベルの機能の動作が上記オーバーレイファイル内の使用許諾契約情報が現在導入されていると自動的に可能になることを特徴とする上記のプログラムファイル使用の制御方法。

10. 上記オーバーレイファイルを上記登録用コンピュータから上記遠隔コンピュータに伝送する以前に、上記使用許諾契約情報を有効化する工程を有する請求の範囲第18項に記載の方法。

10. 不正変更防止になっているオーバーレイファイルを検出する工程を有する請求の範囲第18項に記載の方法。

11. 上記不正変更防止オーバーレイファイルが上記不正変更防止オーバーレイファイルを暗号化キーで暗号化することにより作成され、送付元装置は上記暗号化不正変更防止オーバーレイファイル内に提供するとともに暗号化キーを上記不正変更防止オーバーレイファイルに提供し、上記暗号化キーは暗号化キーは上記オーバーレイファイルの独自の内容によって自動的に決定されることを特徴とする請求の範囲第10項に記載の方法。

上記登録シェルプログラムは使用者が様々な使用許諾契約情報を入力することを可能にするよう少なくとも一度の登録コンピュータと、

登録プログラムと、上記使用許諾契約情報を受信し処理するための手段と、第二レベルの機能を有するプログラムモジュールと使用許諾契約情報の全部あるいは一部を含む独自のオーバーレイファイルを生成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記遠隔コンピュータに伝送することで、上記オーバーレイファイルに入っている使用許諾契約情報が現在使われているときだけ、上記プログラムファイルの第二レベルの機能動作が可能なることを特徴とする上記システム。

28. 上記遠隔コンピュータと上記登録用コンピュータとの間に電子データリンクを有し、ファイル伝送過程で上記登録用コンピュータと上記遠隔コンピュータの両方に備えられていることを特徴とする請求の範囲第17項に記載のシステム。

29. 上記登録用コンピュータが、すべての登録済み使用者が含まれる中央データベースと上記使用許諾契約情報を有効化する手段とを備えていることを特徴とする請求の範囲第27項に記載のシステム。

30. オーバーレイファイルを作成するための上記手段が、送付元装置が記憶されている不正変更防止オーバーレイファイルを作成するための暗号化キーと解読キーとを備えており、上記解読キーは上記オーバーレイファイルと共に上記遠隔コンピュータに伝送され、上記暗号化キーは解読キーはファイルの内容によって自動的に決定されることを特徴とする請求の範囲第27項に記載のシステム。

22. 新しい送付元装置が、上記オーバーレイが実行のためにロードされるたびに更新されて、上記オーバーレイファイルと共に伝送された送付元装置と比較され、上記オーバーレイファイルが作成以降変更されているかどうかを判断することを特徴とする請求の範囲第11項に記載の方法。

23. 上記使用許諾契約情報と上記オーバーレイファイルが、上記登録シェルと上記登録プログラムとの間に電子データリンクを介して伝送されることを特徴とする請求の範囲第18項に記載の方法。

24. 上記登録シェルプログラムが、上記独立登録プログラムを備えた第二のコンピュータから離れている第一のコンピュータに備えられていることを特徴とする請求の範囲第18項に記載の方法。

25. 上記有効化により上記使用許諾契約情報が上記登録シェルを介して有効であることを特徴とする請求の範囲第19項に記載の方法。

26. 上記使用許諾契約情報と上記オーバーレイファイルが同一のコンピュータに入力され、備えられていることを特徴とする請求の範囲第18項に記載の方法。

27. 破壊されたあるいは更新されない期間、プログラムファイルをアップグレードするシステムにおいて、

第一レベルの機能を有するプログラムを含むオーバーレイローダー部分を含むプログラムファイルが最初備わって、上記オーバーレイローダー部分は本物のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記遠隔コンピュータには登録シェルプログラムが備えられ、

テム。

31. 上記遠隔コンピュータが、上記オーバーレイファイルを解読し、上記オーバーレイファイルが実行のためのロードされるたびに新しい送付元装置と計算し、そしてこの装置を上記登録用コンピュータにより上記オーバーレイファイルと共に伝送された送付元装置と比較するための手段を備えていることを特徴とする請求の範囲第30項に記載のシステム。



### 発明の概要を説明

本発明の目的は、許諾者がそのプログラムの費用対効果に関する費用を従来使用されている方法よりはるかに効率的な方法で維持することを可能にすることである。さらに、本発明の第二の目的は、被許諾者あるいは使用者が特定のプログラムの購入あるいは使用許諾を得る際に試行することを可能にすることである。さらに、本発明の更なる目的は、特定のプログラムの使用許諾保護されたアップグレード版を被許諾者に配布する手段を提供することである。したがって、本発明の利点は包括的なものと見えられ、そしてどのようなソフトウェアプログラムも本方法によって配布できるものと意図されている。

一実施例において、動作可能なエグゼクティブ制御ループを除いて完全な製品プログラムが、パーソナルコンピュータあるいは他の装置において、磁気ディスク、フロッピーディスク、ハードウェアあるいは他の手段で最初に提供される。さらに、この特定プログラムには登録シリアルプログラムも含まれる。ただし、小さいプログラムもしくは実行可能なプログラムの場合、プログラム自体は含まれず、シリアルだけが提供される。エグゼクティブ制御ループが除外されているため、このプログラムは正しい複製過程を再現しなければ動作しない。図1および図2に示されているように、この登録過程は、パーソナルコンピュータ(PC) 10内部の登録シリアルプログラム11と登録用コンピュータ12内部に提供されている登録プログラム13とを使用して開始される。登録システムプログラムは登録用コンピュータ13内に提供され、電子データリンク30を通して登録シリアルプログラムがアクセスできる。この電子データリンクは、ローカルエリアネットワークでもよく、電話モデムリンクでもよく、あるいはその他のいかなる種類であってもよい。ただし、第二の実施例においては、登録シリアルおよび登録システムプログラムは同一の媒体上に格納してもよいが、その媒体は製品応用プログラムとは別でなければならない。この場

### 特表平6-501120(5)

合、登録シリアルおよび登録システムプログラムが入っている形態可能な媒体は、許諾された購入プログラムによって使用可能なパーソナルコンピュータ10へ個人的に移植され、電子データリンクは必要ではない。

登録シリアルプログラムは、使用可能なオペレーティングシステム14のメインプログラムファイル内に提供されている製品応用プログラムの実行を最初に許可すると実行される。登録シリアルは、製品応用プログラムに関する追加情報を提供しそれをPC表示装置に表示すると同時に、見込み被許諾者を促して使用者として登録する。使用許諾は、特定の支出場所における特定の被許諾者に対して提供され、その期間は様々な長さもしくは一時的でよく、そのための費用は被許諾者に対して課せられない。ただし、登録シリアルは、不正複製防止オーバーレイファイルが存在しないかぎり、メインプログラムを実行しない。登録シリアルプログラム11は、被許諾者のPCに表示されるデータ入力形式を提供し、被許諾者に対して、請求書送付先、口座番号、使用許諾条件などの個別情報の提供を要求する。この情報は、被許諾者が再確認する登録要求ファイル25に入力される。そして、登録シリアルプログラムは、被許諾者が指定キーを押して登録を開始するのを待つ。このキーが押されると、登録ファイルが読み、そして登録シリアルファイル転送プログラム26が登録システムファイル25と、そのデータリンクを確立する。登録用コンピュータ内の登録プログラム40は、データリンクが正しい登録シリアルで確立されていることを確認する複製保護チェックを実行する暗号化手段によって保護される。つまり、登録シリアルは登録要求ファイル25と、そのファイルを受信する登録システムに転送し、必要な暗号化チェックと、結合されたファイル転送プログラム26および32間のハンドシェイク動作を実行する。完全な登録要求ファイルが中央登録用コンピュータで受信されると、登録要求が登録済み使用者94のデータベースに対して格納される。確認には、その要求に答えるべきかど

うかを判断する様々なチェックが含まれる。たとえば、一時的使用許諾に対する要求が特定の被許諾者から再提供されてきた場合、その被許諾者には使用許可が与えられず、そしてそのプログラムのエグゼクティブ制御ループは過剰されない。そのような状況が発生した場合、適切なメッセージが登録シリアルに転送され、見込み被許諾者に対して表示される。しかし、要求が確認されると、登録済み使用者データベースへの登録が修正されるが、この過程全体が完了するまで、そのデータベースには入力されない。

登録用コンピュータ13の内部では、つぎに使用制御データが使用されて、使用制御データとエグゼクティブ制御ループプログラム命令36とを結合することにより作成された独自の不正複製防止オーバーレイファイルが生成される。結合されたデータとプログラムファイルに基いて、不正複製防止オーバーレイファイル37内に含まれる巡回冗余検査(CRC)値が計算される。一式の独自の暗号化キーと解読キーが作成され、不正複製防止オーバーレイファイルの内容全体が暗号化キーを使用して暗号化される。この暗号化キーに基づき、不正複製防止オーバーレイファイルと共に提供される使用制御キーが提供される。暗号化アルゴリズムは、巡回暗号化システムのように、暗号化と解読にそれぞれ異なるキーを使用する状況であればなんでもよい。登録システムが、不正複製防止オーバーレイファイルと解読キーを、パーソナルコンピュータ10登録シリアルに転送される1個のデータファイル38に格納する。また、更新されたメインプログラムファイルもこのデータファイルに格納され、ファイル転送プログラムとすでに確立されているデータリンクとを基にPCの登録システムに転送される。

出所ファイル形式の受信と同時に、登録シリアルプログラム内の開梱-導入プログラム14が出所ファイルを開き、エグゼクティブ制御ループセグメント16、CRC値22ならびに解読キー20および、含まれている場合は、更新メインプログラムファイルを含む不正複製防止オーバーレイファイル40を導入する。これで登録過程が

完了したので、電子データリンクを切断する。登録データベースレコードが入力され、そして被許諾者の要求に対する請求が、中央登録用コンピュータ12における別のプログラムによって実行される。

登録が終了すると、被許諾者のパーソナルコンピュータに導入された配布済み製品応用プログラムを起動して、不正複製防止オーバーレイファイルと解読キーを使用して製品応用プログラムを実行するたびに実行する製品応用プログラム一式をロードするためのプロセスが開始される。

このプログラム実行過程を図1に示す。図示されているように、パーソナルコンピュータの使用者が製品応用プログラムの実行をオペレーティングシステムに命令すると、オペレーティングシステムはメインプログラムとローダーセグメントをロードする。ローダーセグメントは他のすべてのプログラム命令に先立って実行される。つまり、ローダーセグメントは製品応用プログラムの起動を実行し、不正複製防止オーバーレイの存在をチェックする。不正複製防止オーバーレイが導入されていないければ、ローダーセグメントは終了してオペレーティングシステムに戻るため、メインプログラムファイルの実行が直前に防止される。不正複製防止オーバーレイが導入されている場合、ローダーセグメントは解読キーを見つけて不正複製防止オーバーレイの解読とロードを行ない、メインプログラムファイルに対して存在しないエグゼクティブ制御ループプログラム命令ならびに独自の解読および使用許諾制御データを渡す。解読およびロード過程において巡回冗余検査が実行され、それが完了すると、不正複製防止オーバーレイが登録用コンピュータからパーソナルコンピュータに転送されたときに作成された不正複製防止オーバーレイに記憶された巡回冗余検査値と比較される。巡回冗余検査が失敗に終わると、そのオーバーレイは切りかきの方法によって複製が与えられたものとみなされ、したがって無効とされる。この時点で、ローダーセグメ

## 特表平6-501120 (6)

ントはそのオーバーレイを取り外し、終了してオペレーティングシステムに戻る。したがって、不正変更防止オーバーレイが含まれていない場合と同様に、メインプログラムファイルの実行は、不正変更防止オーバーレイのどの部分が変更されていても、事前に防止される。返戻元長検査の結果、オーバーレイが変更されていないことが確認されると、コードセグメントはオーバーレイを含めたメインプログラムファイルの実行を開始し、そして製品応用プログラムが最後まで実行される。

不正変更防止オーバーレイを動作可能形態の製品応用プログラムに含めることを要求することにより、複製防衛機能と使用許諾制御アーチがそのように動作可能プログラムに共に含まれることになる。このようにして、許諾者は不正使用を防止するとともに監視することが出来る。

図1および図2を参照しながら説明したように、本発明によると、登録過程によって、メインプログラムファイルのニグゼクティブ制御ループセグメントと使用許諾制御データを含む不正変更防止オーバーレイファイルが生成される。登録過程が完了すると、この不正変更防止オーバーレイは登録用コンピュータからパーソナルコンピュータに転送される。この不正変更防止オーバーレイは、起動時に不正使用を防止するキー装置である。なぜなら、ニグゼクティブ制御ループプログラム命令は、独自なしは独自の使用許諾制御データと使用許諾制御データから分離することのできなければ、複製防衛機能と使用許諾制御アーチも複製なしには複製できないからである。

この不正変更防止オーバーレイファイルは、オーバーレイファイルが印加される時に最初に返戻元長検査値をオーバーレイファイルに記憶させると不正変更防止になるとみなされる。返戻元長検査値は、プログラム命令と使用許諾データを含むオーバーレイファイルの内部全体に対して計算される。複製防衛データは製品であるので、各々のCRCは独自なものになる。記憶されてい

るCRC値が、オーバーレイがロードされるたびにローダーセグメントによって計算された返戻元長検査値と比較される。これらの返戻元長検査値が一致しなければ、ローダーセグメントは終了してオペレーティングシステムに戻る。したがって、オーバーレイファイルの内容にどんな変更が加えられていれど、記憶されている返戻元長検査値に付随する変更が行われない限り、そのオーバーレイファイルは無効になる。つぎに、不正変更防止オーバーレイの内容全体が、返戻元長検査値の位置が不明になるような方法で暗号化されるので、この値の存在をいつとてそれを変更することが困難になる。

また、暗号化により、不正変更防止オーバーレイに含まれる特定のプログラム命令ならびに独自の使用許諾制御および使用許諾制御データがはつきりしくなる。暗号化は、公開鍵暗号化システムのように暗号化と復号に別々のキーを使用する成法によって達成される。暗号化ならびに独自の暗号化キーおよび解読キー発生のためのアルゴリズムは登録システム内に蓄積し、したがって複製防衛にはアクセスが不可能である。解読キーは、登録システムと登録プログラムシェルのを通じて複製防衛者のコンピュータに伝送される。オーバーレイファイルを解読するためのアルゴリズムはローダーセグメント内にあるので、解読キーと解読アルゴリズムを使用してオーバーレイファイルを解読しその内容を検査することは、困難ではあるが可能である。しかし、内容を複製して、新しい複製されたオーバーレイファイルを暗号化する試みに、暗号化キーに対するアクセスができないために阻止される。私的暗号化キーで暗号化されたオーバーレイファイルだけでは複製防衛システムで解読できず、私的キーは公共キーから複製には用いられないというのが、公開鍵暗号システムの特徴である。

不正変更防止オーバーレイファイルは、プログラム命令のエグゼクティブ制御ループセグメントと、使用許諾の方法と制御に適切な独自の使用者識別データとを有している。このデータには、

使用許諾の期限、コンピュータの製造番号、コンピュータのモデルの電路番号、そしてその他の情報が含まれる。

ローダーセグメント18は登録目的のサブプログラムであり、これは、ローダープログラムが取り除かれたり返戻された場合、メインプログラムファイルを動作可能にする方法によって製品応用プログラムのメインプログラムファイルに結合される。この結合状態は、特定のプログラム命令と製品応用プログラムのメインプログラムファイル内部に内蔵するプロセスである。これらの内蔵された命令は、使用者にとっては未知の記憶位置にある特定の値を検査する。ローダープログラムセグメントを実行すると、特定の値がメインプログラムファイルの動作を可能にするのに必要な特定の記憶アドレス位置に記憶される。ローダープログラムセグメントは、その他の機能の他にこの動作を実行する。したがって、ローダーセグメントを取り外したり返戻したりすると、メインプログラムファイルには特定の位置における特定の値が含まれないことになり、そのため動作不能になる。

図の実施例において、登録シェルは、製品応用プログラムの動作可能なデモンストレーション版を含んでいる可能性があるマーケティングパッケージの一部として配布される。デモンストレーション版のプログラムは、ローダーセグメント、デモンストレーション版の解読キー、そしてデモンストレーション版の不正変更防止オーバーレイを含むように設計されている。この場合、不正変更防止オーバーレイには独自の使用許諾データは含まれないが、登録版の製品の複製と表示のデモンストレーションだけを許なうメインプログラムエグゼクティブ制御ループが含まれるであろう。デモンストレーション版のエグゼクティブ制御ループは、エグゼクティブ制御ループの複製設計によって複製されたプログラムの様々な機能を有している。たとえば、複製版を複製するデモンストレーションメニューをプログラミングして返戻版を複製することが出来るが、デモンストレーション版のエグゼクティブ

制御ループをプログラミングして返戻版を製品登録依頼として複製して、製品を制作させる前に登録することを要求できる。

登録を開始する前に、見込み版の複製はプログラムを実行し、デモンストレーション版が実行されであろう。前述しそして図2に示したように、デモンストレーション版の解読キーが使用され、デモンストレーション版のエグゼクティブ制御ループがロード、解読、そして実行される。デモンストレーションが終了すると、見込み版の複製は、使用者として登録し登録版のプログラムを執行するための一時的な使用許諾を得るようになれる。そして、使用者は前述のようにして登録を行い、図2に示されているプロセスを開始することが出来る。登録要求に回答して、新しいオーバーレイファイル40'と独自の解読キー20'が含まれている応答ファイルが登録用コンピュータから送られる。追加プログラムファイルと更新版のプログラムファイルも、応答ファイルと共に受信される。登録プログラムはデモンストレーション版の不正変更防止オーバーレイ40と解読キー20とそれぞれ登録版40'と10'で置き換える。

登録に続き、使用者がプログラムを実行すると、プログラム実行過程で登録済み版の不正変更防止オーバーレイ40'が検出されてロードされ、独自の解読キー20'を使用することにより、登録済み版のエグゼクティブ制御ループが解読され実行される。このようにして、デモンストレーション版は完全に動作する登録版に置換される。

プログラムの複製向上版が利用される場合、使用者は同一のプロセスを起動してさらに別の解読キーと、より強化されたニグゼクティブ制御ループと追加プログラムファイルとを有する別の不正変更防止オーバーレイとを受領して、より強化された版の製品に更新することが出来る。

様々な実施例が、小さな不正変更防止オーバーレイを使用して大きなプログラムの制御を行なうための連続で動的な複製を促

特表平6-501120 (7)

用することができる。このような状況は、ここにも含まれているように、プログラムの部分あるいはプログラム全体を使用済領域と結合する形式で配相するための、ここに開示されている方法がもたらす商業的利便の可成りの早なる例である。

上記の知見に照らし合わせ、本発明は様々な変形例が可能なのは明らかである。たとえば、本発明は、使用者のコンピュータがその地域の登録用コンピュータに接続され、あるいはその登録用コンピュータがそれより広い地域の登録用コンピュータに接続され、というように階層構造的に実施することも可能である。その地域の登録用コンピュータの登録領域は、その地域の登録用コンピュータとそれより広い地域の登録用コンピュータとの契約に含まれる使用許諾制御ゲートによって制御できるであろう。したがって、下記の発明の範囲内であれば、本発明を上記明細書に記載されている以外の方法で実施することができる。

図 1

発明過程

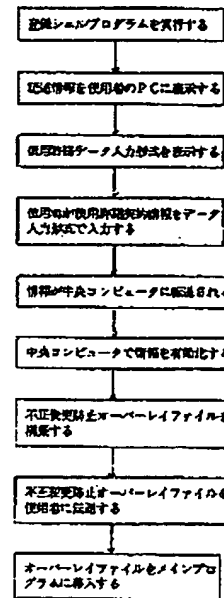
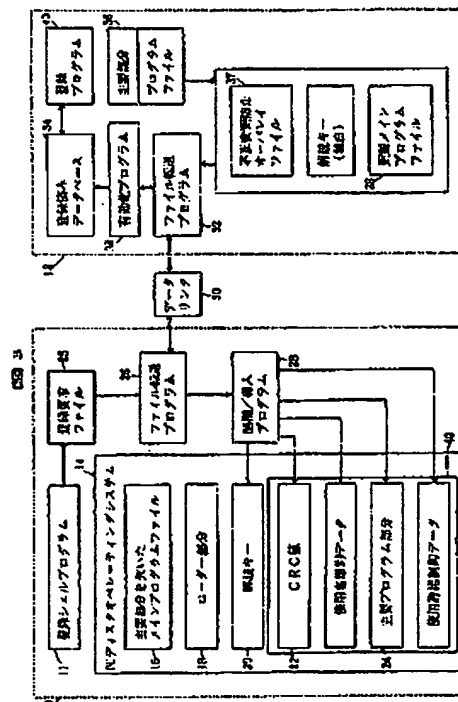
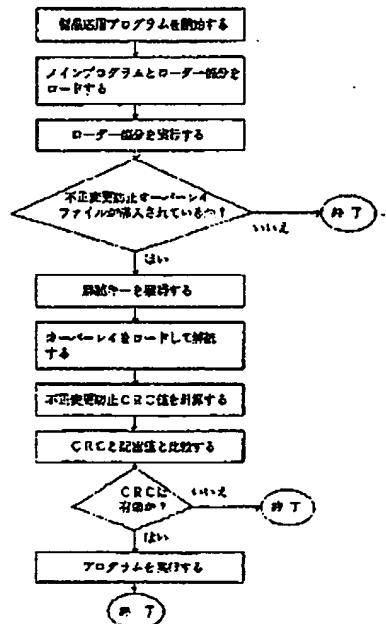
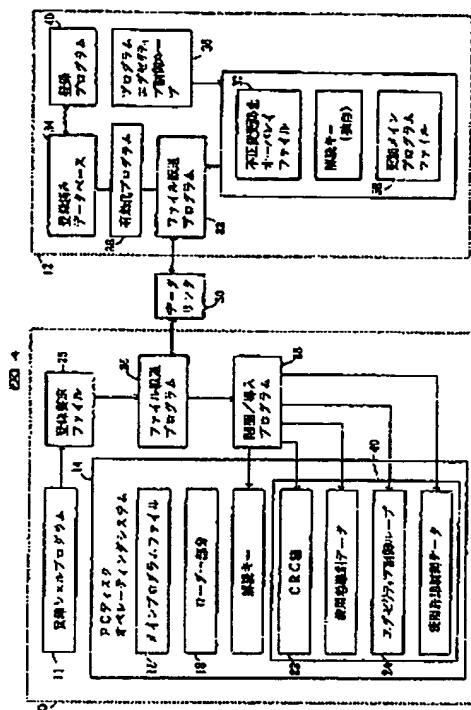


図 2

プログラム実行過程





[illegible]

(51) Int. Cl.<sup>5</sup>                      識別記号                      庁内整理番号                      F 1  
H 0 4 L   9/12

(61) 指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IT, LU, NL, S E), CA, JP